CINDY A. COHN (SBN 145997)
cindy@eff.org
MARCIA HOFMANN (SBN 250087)
marcia@eff.org
HANNI FAKHOURY (SBN 252629)
hanni@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Fax: (415) 436-9993

Attorneys for *Amicus Curiae*
Electronic Frontier Foundation

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

FACEBOOK, INC., Plaintiff, v. POWER VENTURES, INC., Defendant.	Case No. 5:08-cv-05780 JW **BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT POWER VENTURES' MOTION FOR SUMMARY JUDGMENT ON COUNT 1 (CAN-SPAM ACT, 15 U.S.C. § 7704) AND UNDER CALIFORNIA PENAL CODE § 502 AND THE COMPUTER FRAUD AND ABUSE ACT** Date: January 23, 2012 Time: 9:00 a.m. Courtroom 9, 19th Floor Hon. Judge James Ware

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES

STATE STATUTE

OTHER AUTHORITIES

TREATISES

LEGISLATIVE MATERIALS

STATEMENT OF INTEREST OF AMICUS CURIAE

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported digital civil liberties organization. As part of its mission, EFF has served as counsel or amicus in key cases addressing user rights to free speech, privacy, and innovation as applied to the Internet and other new technologies. With more than 16,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at www.eff.org.

EFF has already assisted the Court in this case by filing two amicus briefs regarding Facebook's claim under California Penal Code § 502(c). (Dkt. Nos. 78-1 & 83.) EFF has also helped other courts to interpret and apply computer crime statutes to modern communications technologies in cases such as *United States v. Drew*, 259 F.R.D. 449, 465 (C.D. Cal. 2009); *United States v. Nosal*, 642 F.3d 781 (9th Cir. 2011), *rehearing en banc granted*, 661 F.3d 1180; and *United States v. Cioni*, 649 F.3d 276 (4th Cir. 2011).

EFF's continuing interest in this case is the sound, principled and fair application of the law to online activities and systems, especially as the law affects both the users of online systems and the innovators who improve the experience of users. EFF is especially concerned about Facebook's core claim: that Facebook users who chose to use third parties to automate access to their information stored with Facebook expose the third parties that assist them, and potentially themselves, to serious civil and criminal liability. Here the liability arises from Facebook's claims under California's computer crime statute (California Penal Code § 502), and the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and the CAN-SPAM Act (15 U.S.C. § 7704).[1]

[1] EFF notes that it was allowed access only to to redacted versions of the briefs and only in in late December. EFF has not had access to all of the underlying evidence. As a result, EFF cannot comment on several of the arguments and facts presented to the Court by the parties.

I. INTRODUCTION AND FACTS

A. Summary of the Argument

Facebook's claims in these cross summary judgment motions are all based on a single underlying theory. Facebook contends that because Power's service enabled Facebook users to automate actions using their own data that they could have performed themselves manually, Power has violated the law. In the case of the Computer Fraud and Abuse Act ("CFAA") and California Penal Code § 502(c), the user had to provide her own valid username and password through Power to obtain access to Facebook and her own social networking data. In the case of the CAN-SPAM Act, the user had to affirmatively opt in to a promotion to allow Power to automate Facebook's Event invitation feature. In both contexts, Facebook's claims are legally wrong and dangerous as a matter of policy, thwarting consumer choice and giving service providers the power to manufacture and cherry-pick anti-competitive lawsuits against follow-on innovators.

Facebook encourages the Court to interpret particular phrases in the CFAA and section 502(c) to give those statutes a broad application, which is particularly concerning because those statutes are primarily criminal laws. Facebook's reading of these statutes would not only stifle innovation, but also create legal uncertainty and the risk of capricious enforcement. This Court should reject Facebook's claims to avoid rendering these laws unconstitutionally vague.

Facebook's CAN-SPAM claims appear to be based wholly on Facebook's decision to design and implement its captive Event invitation feature. As a result, Facebook's claim, if accepted by this Court, would allow Facebook or any other creator of a "captive" email generation system to impose the CAN-SPAM Act's strong punitive scheme on any commercial uses of the creator's system that displease it.

In sum, Power's servers only connected with the user's data on Facebook servers, and only sent out Event invitations, *at the behest of an authorized Facebook user*. While users who choose to automate access to their own data may breach Facebook's terms of use (if those terms are otherwise enforceable), breaches of these sorts of private contracts should not amount to criminal conduct, for either the user or for the provider of the automation tool. This is especially the case when Facebook has breach of contract remedies available to it, including termination of a

misbehaving user's credentials. For these reasons, EFF urges the Court to grant summary judgment in favor of Power on Facebook's claims under the California Penal Code, CFAA, and CAN-SPAM Act.

B. Facebook's Service

Facebook allows its users to store their own information on Facebook's servers using Facebook's web interface for uploading and viewing information. This interface allow Facebook users to make lists of friends, publish status updates, post photographs and videos, create common interest groups, and manage pages on behalf of organizations and public figures.[2] It also allow users to create virtual and actual "events" and invite their friends to attend.

Facebook has been wildly successful at acquiring users. The service currently claims more than 800 million active users,[3] and over 50% of its active users—over 400 million people—log on to Facebook in any given day.[4] As of April 2011, one in eleven humans on the planet were on Facebook.[5]

Facebook is also an aggressively commercial service, a leader in what has been called "social commerce. " Facebook encourages companies to leverage Facebook users' social networks to make commercial sales. In fact, Facebook's role in this commercial world is so powerful that it has its own name, "f-commerce."[6] Top brands on Facebook include such household names as Coca-Cola, Disney, Starbucks and Oreos.[7] The commercial activity on Facebook includes use of the Events feature.

Importantly, Facebook users own the information they store with the company. The

---

[2] Facebook Factsheet, http://www.facebook.com/press/info.php?factsheet (last visited Jan. 9, 2012).
[3] Facebook Statistics, http://www.facebook.com/press/info.php?statistics (last visited Jan. 9, 2012.)
[4] *Id.*
[5] Paul Marsden, *F-Commerce Statistics Roundup: Facebook Commerce by the Numbers*, Social Commerce Today, April 4, 2011, http://socialcommercetoday.com/f-commerce-statistics-roundup-facebook-commerce-by-the-numbers/.
[6] Paul Marsden, *The F-Commerce FAQ: All You Ever Wanted to Know About Facebook Commerce But Were Afraid to Ask*, Social Commerce Today, April 28, 2011, http://socialcommercetoday.com/f-commerce-faq-all-you-ever-wanted-to-know-about-facebook-commerce-but-were-afraid-to-ask/.
[7] *Facebook Facts and Figures*, Website Monitoring Blog, Oct. 14, 2011, http://www.website-monitoring.com/blog/2011/10/14/facebook-facts-and-figures-2011-infographic/.

company's terms of service at all times relevant to this case confirm this fact and it is not disputed here.[8] Ownership and control are extremely important to Facebook users, as the company learned in February 2009 when it modified its terms of use to give Facebook the right to continue to use content indefinitely even after a user attempted to delete it or leave the service altogether. After a huge outcry, the company backpedaled, and reinstituted the old terms that allowed users to delete their content from the site.[9]

As part of its business model, Facebook has steadily increased the amount of information about its users and their activities it offers to third parties for commercial and noncommercial use. Facebook has several Application Programming Interfaces, or APIs, through which third parties can see the information and activities of Facebook's users. Through controversial changes to its terms of service and the functionality of its API, Facebook offers to certain third parties and advertisers as much information about any particular user and his or her friends as that user personally could have accessed using Power's service.[10] Thus, by continuing to press for Power to be liable under criminal law, Facebook's actions appear to be aimed not at protecting users from the sharing of their information with third parties, or at preventing commercialization of its service, but at ensuring Facebook's own control over (and the corresponding ability to monetize) user information, even against the users themselves.

---

[8] Facebook's Statement of Rights and Responsibilities confirms: "You own all of the content and information you post on Facebook" and "[f]or content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it." Facebook Statement of Rights and Responsibilities § 2 (last revised Jan. 11, 2012), https://www.facebook.com/legal/terms.

[9] Bill Meyer, *Facebook Data-Retention Changes Spark Protest,* Feb. 17, 2010, http://www.cleveland.com/nation/index.ssf/2009/02/facebook_dataretention_changes.html.

[10] *See*, *e.g.*, Erick Schonfeld, *Microsoft Taps Into Facebook's Open Graph to Launch Docs.com* (April 21, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/04/21/AR2010042103128.html; Matt Rosoff, *Pandora and Facebook Get Social Music Right* (Apr. 22, 2010), http://news.cnet.com/8301-13526_3-20003210-27.html.

C. Power's Service

Power provided a service that enabled individuals with valid accounts on multiple social networks to aggregate their information stored with each network, giving them the ability to view their data and friend lists, as well as other information, across multiple services on a single screen. The user could then click through the Power.com interface to go to any of her social networks and interact with them through that network's user interface. Power's service was a follow-on innovation to social networking services, giving the user more options to view and use her own information stored with them. For instance, Power.com allowed a user to see all of her friends and contacts in a single list, regardless of which social networks they used. Power also offered the user a tool by which she could easily export her information from social networks into a spreadsheet format, thus aiding users who might want to move their information from one social network to another. Power stopped providing its service to Facebook users in early 2009, after this lawsuit was filed. 12/2/11 Steve Vachani Decl. ¶ 13 (Dkt. No. 189).

D. Facebook's IP Blocking Effort

In December 2008, Facebook and Power conferred about Power's implementation of user access to Facebook accounts. Apparently Facebook wanted Power to use Facebook's API rather than connect a user directly to her account information so that Facebook would have more control over how stored data was accessed and manipulated, but Power felt that the API did not allow the full functionality Power wanted to bring to its customers.[11] During these negotiations, Facebook blocked a single Internet Protocol (IP) address that Power's server had used in the past.[12] 12/2/11

[11] EFF takes no position on this question. Facebook may have valid reasons for wanting application developers to go through its API, and Power and its users may have had valid reasons for wanting the ability to exercise more control over users' data. Two businesses can have valid but competing views about which tools are valuable to their user bases, which is another reason why imposing criminal liability or severe civil penalties like CAN-SPAM's treble damages is wholly inappropriate in these kinds of disputes.

[12] As described in detail in EFF's June 21, 2010 amicus brief and declaration of Seth Schoen, Dkt. Nos. 83 and 84, IP blocking is simply a method of preventing a computer with one IP address from connecting to another. This technique has no bearing on computers associated with any other IP address or individual users who connect to the internet using different machines or access points. If the person originally using the blocked IP address changes to a different IP address for any reason, the block will not affect her any longer.

Steve Vachani Decl. at ¶¶ 10-11; *see also* Steve Vachani Decl. ISO Power Opp. to Mot. J. on the Pleadings or Partial Summ. J. at ¶ 9 (Dkt. No. 65). This attempt was ineffective, however, because Facebook did not block any IP address that Power's server was actually using at the time. 12/2/11 Steve Vachani Decl. at ¶¶ 10-13.

Facebook does not claim that Power actually disabled or circumvented its IP block, nor that the service did any damage to Facebook's servers. Rather, Facebook contends that Power designed its service to rotate IP addresses so that its servers would not be blocked at some point in the future if Facebook attempted to prevent Power users from accessing their own Facebook accounts through the Power interface. Facebook Opp. to Power Mot. Summ. J. at 2-4 (Dkt. No. 187); Facebook Mot. Partial Summ. J. on § 502(c) & CFAA (Dkt. No. 168). Thus, Facebook's claims under California Penal Code § 502(c) and the CFAA now rest primarily on Power's design decisions rather than on an act of circumvention.

E. Power's Promotional Event

As part of Power's effort to market its service, Power offered a promotion to users who also had Facebook accounts. Power advertised to its users that, if they chose to invite their friends to try Power's system, they could win $100. The promotion displayed a pop-up box that said: "share with friends through events." Facebook Corrected Mot. Partial Summ. J. on Count 1 at 5:13-21 (Dkt. No. 174). While the specific "event" checkbox on the promotion was pre-checked, consent to participate in the campaign overall required an affirmative click by Power's users.[13] When those users chose to participate in the promotion, Power automated the process of inviting the user's Facebook friends to join Power's service through Facebook's captive "events" interface, which, as described further below, prevented Power (and the user) from changing key elements of the invitation.

[13] EFF generally disapproves of pre-checked boxes as not a true opt-in, but they are ubiquitous. Facebook uses them in many places on its system, including its own privacy settings.

II. ARGUMENT

A. POWER HAS NOT VIOLATED CALIFORNIA PENAL CODE SECTION 502(C) OR THE FEDERAL COMPUTER FRAUD AND ABUSE ACT.

1. California Penal Code § 502 and the Computer Fraud and Abuse Act are Criminal Statutes, and Must be Narrowly Interpreted to Avoid Vagueness.

While this is a civil case, California Penal Code § 502 and the Computer Fraud and Abuse Act are primarily criminal laws. Facebook urges the Court to interpret them expansively, but as the Supreme Court has observed, courts must adopt a narrow construction of a criminal statute to avoid vagueness. *See United States v. Skilling*, __ U.S. __, 130 S. Ct. 2896, 2927-28 (2010); *Kolender* v. *Lawson*, 461 U.S. 352, 357 (1983). As explained below, Facebook's urged constructions would fail to put people on adequate notice about which conduct is criminally prohibited, and enable the government to enforce the law in an arbitrary and discriminatory manner.

A plurality of the Supreme Court has specified that "[v]agueness may invalidate a criminal law for either of two independent reasons. First, it may fail to provide the kind of notice that will enable ordinary people to understand what conduct it prohibits; second, it may authorize and even encourage arbitrary and discriminatory enforcement." *Chicago v. Morales*, 527 U.S. 41, 56 (1999) (Stevens, J., plurality opinion); *see also Grayned v. Rockford*, 408 U.S. 104, 108-09 (1972). In *Grayned*, the court explained:

> [I]f arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them. A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application. In the Ninth Circuit, "[t]o survive vagueness review, a statute must '(1) define the offense with sufficient definiteness that ordinary people can understand what conduct is prohibited; and (2) establish standards to permit police to enforce the law in a non-arbitrary, non-discriminatory manner.' *United States v. Sutcliffe*, 505 F.3d 944, 953 (9th Cir. 2007) (quoting *Nunez v. City of San Diego*, 114 F.3d 935, 940 (9th Cir. 1997).

408 U.S. at 108-09. Unless construed narrowly to satisfy this standard, the statutory provisions at issue here could be invalidated for both reasons.

The impact of a broader construction here would be significant. Should the Court accept Facebook's view of the violation of Terms of Use alone as a violation of the CFAA, millions of otherwise innocent innovators and computer users commit frequent criminal violations of the law

through ordinary—indeed routine—online behavior everyday. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act,* 94 MINNESOTA LAW REV. 1561 (2010). And if the Court accepts Facebook's novel theory for pre-circumvention of a technical measure, a large number of innovators would be at risk for developing follow-on products and services to enable users to interact with their own data in new and exciting ways.[14] In either case, the public would be unable to distinguish in a meaningful and principled way between innocent and criminal activity, which is a constitutional harm. *Humanitarian Law Project v. Mukasey*, 509 F.3d 1122, 1133 (9th Cir. 2007).

2. Violating Terms of Use Does Not Constitute Unauthorized Access Under The Computer Fraud and Abuse Act.

As this Court has already determined, breaching terms of use alone does not violate California Penal Code § 502(c). *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08-05780, 2010 U.S. Dist. LEXIS 93517 (N.D. Cal. July 20, 2010). This Court rightly noted, "interpreting the statutory phrase 'without permission' in a manner that imposes liability for a violation of a term of use or a receipt of a cease and desist letter would create a constitutionally untenable situation in which criminal penalties could be meted out on the basis of violating vague or ambiguous terms of use." *Id.*, 2010 U.S. LEXIS 93517, *35. Despite this clear ruling, Facebook maintains that violating terms of use constitutes "unauthorized access" for purposes of the CFAA. Facebook Mot. Partial Summ. J. on § 502 & CFAA at 4:10-14.

For the same reasons at the Court identified in its prior ruling on Penal Code § 502(c), breaching terms of use cannot render access unauthorized under the CFAA. 18 U.S.C. § 1030(a)(2)(C) makes it illegal to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer." Under 18 U.S.C. § 1030(a)(4), it is unlawful to "knowingly and with intent to defraud, access[] a

[14] EFF notes that the term "circumvention" can be misleading in this context, since the CFAA does not speak in those terms. Yet we note that even the Digital Millennium Copyright Act, which actually does seek to prevent some kinds of circumvention of technological measures protecting copyrighted works, contains an exception to ensure that independently created computer programs can interoperate with existing computer programs. 17 U.S.C. § 1201(f).

protected computer without authorization, or exceed[] authorized access, and by means of such conduct further[] the intended fraud and obtain[] anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period[.]" Both provisions carry civil and criminal penalties, and all violations of subsection 1030(a)(4) are felonies. 18 U.S.C. §§ 1030(c)(2)-(3).

As EFF pointed out in its May 3, 2010 and June 21, 2010 amicus briefs,[15] Courts have relied on CFAA precedent for guidance when interpreting California Penal Code § 502(c). *See, e.g., Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc*., 556 F. Supp. 2d 1122, 1131-32 (E.D. Cal. 2008) (Because section 502(c) "has similar elements to § 1030" and both parties had "incorporate[d] by reference their arguments regarding § 502 into the arguments regarding § 1030," the court considered the two claims in tandem); *In re Apple & AT&T Mobility Antitrust Litigation*, 596 F. Supp. 2d 1288, 1309 (N.D. Cal. 2008) (court's decision on section 502(c) relied on the exact same "reasons discussed in those prior sections" about the plaintiffs' section 1030 claims). Since the analysis under the California Penal Code and the CFAA is the same, and rather than repeat the reasons that the CFAA is not violated here, EFF urges the Court to review EFF's arguments in its prior amicus briefs and hold that breaching web site terms of use and receipt of cease-and-desist letters does not render subsequent access unauthorized under the CFAA.

EFF notes that the Ninth Circuit is currently reviewing a case that may be relevant here. *United States v. Nosal* raises the question of whether an individual violates the CFAA by accessing a computer for a purpose that violates an employer's corporate policy. In that case, Senior Judge Patel of this Court relied on *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009) to hold that an ex-employee of an executive search firm did not violate the CFAA when he induced current employees to use their legitimate credentials to access a company database and provide him with proprietary information in violation of the employer's computer-use policy. No. 2010 U.S. Dist. LEXIS 24359 (N.D. Cal. Jan. 6, 2010). A Ninth Circuit panel reversed *Nosal*, 642 F.3d 781, and *en*

[15] These amicus briefs are available at docket numbers 78-1 & 83.

banc review was granted, 661 F.3d 1180. EFF has also participated as amicus in that case and believes that the district court's conclusion was correct. However, it may be most prudent for the Court to wait for the Ninth Circuit to rule in *Nosal* before addressing the CFAA issues here.[16]

3. Creation of a Tool That Could be Used to Circumvent a Technological Barrier That Does Not Exist is Not a Criminal Act.

While the Court found that Power could not have violated California Penal Code § 502(c) on the basis of a terms-of-use violation, it left open the possibility that Power might have broken the law if it actually "circumvented Facebook's technical barriers"—specifically, the IP block. *Facebook,* 2010 U.S. Dist. LEXIS 93517 at *36. EFF argued at length in its June 21, 2010 amicus brief that when a person is authorized to access information, as Facebook users unquestionably are, mere circumvention of an IP block to access that information should not per se constitute a criminal act.[17]

Now, however, the circumstances in this case have changed. After discovery and despite its earlier allegations, Facebook is apparently unable to show that Power actually bypassed an IP block or any other technical barrier. In an attempt to salvage its claims, Facebook now argues that Power should be subject to liability under a law with criminal penalties because it designed its product to use multiple IP addresses to access Facebook's servers—well before Facebook ever imposed an IP block. Facebook Mot. Partial Summ. J. on § 502 & CFAA at 5-6; Facebook Opp. to Power Mot. Summ. J. at 2-5; Facebook Reply ISO Mot. Partial Summ. J. on § 502 & CFAA at 2-4. In other words, Facebook claims that the mere creation of a tool that *could be used* to circumvent a technical barrier—even if a technical barrier doesn't exist—creates liability under the California Penal Code and the CFAA.

---

[16] EFF notes, however, that even if the CFAA could be violated by breaching a specific employment contract or policy, that would not necessarily settle the question of whether breach of a mass-market contract of adhesion such as Facebook's terms of service should similarly trigger criminal penalties.

[17] EFF urges the Court to consider those arguments again, since other courts are beginning to rely on that analysis, but will not repeat them except to emphasize that there is nothing inherently improper, much less unlawful, about switching IP addresses and thereby avoiding IP address blocking. Any internet user may have valid reasons for doing so, and the means of switching are common and unremarkable.

Writing code that is capable of circumventing a technical barrier, but never actually does so or even *attempts* to do so, cannot make access "without permission" or "unauthorized." As the Ninth Circuit has held, the computer owner bears the responsibility of actually creating barriers to put others on notice that access is "unauthorized." *Brekka*, 581 F.3d at 1135 ("The plain language of the statute . . . indicates that 'authorization' depends on actions taken by the [computer owner].") Authorization does not turn on the mental state of the party accessing the computer, as Facebook suggests, and as the cases rejecting the breach-of-contract theory of CFAA liability make clear.[18] Such a holding would make it a "thought crime" to produce a tool capable of circumventing any technical barrier another service might create in the future.

Facebook's argument is an extremely broad theory that, if accepted, would chill follow-on innovators who seek to create tools that could potentially be used to circumvent technological barriers, regardless of whether that design choice was innocent or ill-intentioned.[19] They would be forced to anticipate every technical block that any interoperable system or program might possibly impose, then avoid building any tool that could possibly bypass those measures. This is an unworkable rule that cannot pass constitutional muster and would render these computer crime provisions void for vagueness under *Skilling*, *Kolender* and other precedent described above in Section II.A.1.

4. Section 1030(a)(4) of the Computer Fraud And Abuse Act Prohibits Theft, And Power Has Not Stolen Data or Otherwise Interfered With Any Property Right.

While Facebook's claim under 18 U.S.C. § 1030(a)(4) fails because Power did not obtain unauthorized access to Facebook's servers, it also fails because Power did not have "intent to defraud" within the meaning of the statute. Facebook argues that the phrase "simply means wrongdoing, and does not require proof of common law fraud." Facebook Opp. to Power Mot. Summ. J. at 5; Facebook Reply ISO Mot. Partial Summ. J. on § 502 and CFAA at 9-10 (citing

[18] EFF discussed these cases in detail in its May 3, 2010 and June 21, 2010 amicus briefs, and urges this Court to review that precedent.

[19] Note that subsection 1030(a)(2)(C) prohibits "intentionally access[ing] a computer without authorization or exceeds authorized access, and thereby obtain[ing] . . . information from any protected computer." No malicious intent is needed to violate this statute.

Multiven, Inc. v. Cisco Sys., Inc., 725 F. Supp. 2d 887, 892 (N.D. Cal. 2010); *Hanger Prosthetics & Orthotics,* 556 F. Supp. 2d at 1131. Settled Ninth Circuit case law and the CFAA's legislative history require a different conclusion.

The Supreme Court has made clear that "where a federal criminal statute uses a common-law term of established meaning without otherwise defining it, the general practice is to give that term its common-law meaning." *United States v. Turley*, 352 U.S. 407, 411 (1957); *see also United States v. Doe*, 136 F.3d 631, 634 (9th Cir. 1998) ("[i]f Congress uses a common-law term in a federal criminal statute without defining it, we must presume Congress adopted the common-law definition of that term.") (quoting *United States v. Gullet*, 75 F.3d 941, 947 (4th Cir. 1996), *cert. denied*, 519 U.S. 847 (1996) (quotation marks omitted)).

By using the phrase "intent to defraud" in the CFAA, Congress has specifically chosen to criminalize more than just "wrongdoing." It has invoked common-law "fraud." *See United States v. Mead*, 426 F.2d 118, 123 (9th Cir. 1970) ("[i]ntent to defraud has always been an essential element of common law fraud."). The Ninth Circuit has looked at the phrase "intent to defraud" in criminal statutes before and found that Congress intended to capture common-law fraud by using that specific language.

In *United States v. Watkins*, 278 F.3d 961 (9th Cir. 2002), the Ninth Circuit found that 21 U.S.C. § 333(a)(2), a statute that criminalized the misbranding of food or drugs "with the intent to defraud or mislead" included the common-law requirement of materiality even though the statute did not explicitly include a materiality requirement. 278 F.3d at 964. The Court reached this conclusion by relying on the Supreme Court's decision in *Neder v. United States*, 527 U.S. 1 (1999). *Neder* interpreted the phrase "scheme or artifice to defraud" in the federal mail and wire fraud statutes and noted that "none of the fraud statutes defines the phrase 'scheme or artifice to defraud,' or even mentions materiality" and thus "based solely on a 'natural reading of the full text,' materiality would not be an element of the fraud statutes." *Neder*, 527 U.S. at 20-21; *see also Watkins*, 278 F.3d at 965. Yet, as *Watkins* pointed out, the "Court's analysis . . . did not end with this literal reading of the statutory language." *Watkins*, 278 F.3d at 965. Instead, the Supreme Court looked at the common-law meaning of the word "defaud" because of the "well-established rule of construction that '[w]here Congress uses terms that have accumulated settled meaning under the . . . common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of those terms.'" *Id.* (quoting *Neder*, 527 U.S. at 21); *see also Nationwide Mut. Ins. Co. v. Darden*, 503 U.S. 318, 322 (1992). Relying on *Neder*, the

Ninth Circuit in *Watkins* applied the common-law meaning of the word "fraud" to the identical phrase found in the CFAA: "intent to defraud."[20] The same result should apply here.

By using the term "intent to defraud," Congress specifically intended to capture common-law fraud, which is "obtaining money or property by means of false or fraudulent pretenses, representation, or promises." *McNally v. United States*, 483 U.S. 350, 358 (1987) (quoting *Hammerschmidt v. United States*, 265 U.S. 182, 188 (1924)) (quotations omitted).[21] If Congress had wanted the CFAA to cover only "wrongdoing," it would not have used the words "intent to defraud" and invoked the common-law history and definition that goes along with that phrase.

The legislative history of the CFAA supports this conclusion, as well. Congress made clear that it intended subsection 1030(a)(4) to cover instances of theft rather than mere trespass: "[T]here must be a clear distinction between computer theft, punishable as a felony, and computer trespass, punishable in the first instances as a misdemeanor. The element in new paragraph (a)(4), requiring a showing of intent to defraud, is meant to preserve that distinction, as is the requirement that the property wrongfully obtained via computer furthers the intended fraud." S. Rep. No. 99-432, 99th Cong., 2d Sess. (1986), reprinted at 1986 U.S.C.C.A.N. 2479, 2488; *see also* 132 Cong. Rec. 7128, 7129 99th Cong., 2d Sess. (1986); *accord United States v. Czubinski*, 106 F.3d 1069, 1078 (1st Cir. 1997); *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 509 (3d Cir. 2005). The Senate Judiciary Committee also specified that "[t]he scienter requirement for [subsection 1030(a)(4)], 'knowingly and with intent to defraud,' is the same as the standard used for 18 U.S.C. § 1029 relating to credit card fraud." S. Rep. No. 99-432, 1986 U.S.C.C.A.N. at 2488.

While the phrase is not defined in that statute, the Senate Appropriations Committee specified in the legislative history of section 1029 two years before:

---

[20] Similarly, when Congress expressly omits the phrase "intent to defraud" from a statute, the common-law requirements of fraud are not elements of the crime. *See United States v. Reich*, 479 F.3d 179, 187 (2d Cir. 2007) (18 U.S.C. § 505 does not require an intent to defraud absent explicit language in the text of the statute) (Sotomayor, J.); *United States v. Cowan*, 116 F.3d 1360, 1362-63 (10th Cir. 1997) (same).

[21] *McNally* held that theft of *intangible* goods and service, known as "honest services fraud" was not a violation of the wire fraud statute, 18 U.S.C. § 1341. *McNally*, 483 U.S. at 361. Following that decision, Congress attempted to overruled *McNally* by amending 18 U.S.C. § 1346 to define "scheme or artifice to defraud" as to include depriving "another of the intangible right of honest services." *See Skilling*, 130 S. Ct. at 2927. *Skilling* found that portion of section 1346 potentially vague and thus limited honest services fraud to cover only "bribe-and-kickback" schemes. *Id.* at 2931.

> A person engages in conduct knowingly where he is aware of the nature of his conduct and is aware or believes that the item involved in a fraudulent payment device. "With intent to defraud" means that the offender has a conscious objective, desire or purpose to "deceive another person, and to induce such other person, in reliance upon such deception, to assume, create, transfer, alter or terminate a right, obligation, or power with reference to property."

S. Rep. No. 98-368, 98th Cong., 2d. Sess. (1984), reprinted at 1984 U.S.C.C.A.N. 3647, 3650. This definition is consistent with the Senate Judiciary Committee's intent that subsection 1030(a)(4) prohibit theft, not mere trespass. S. Rep. No. 99-432, 1986 U.S.C.C.A.N. at 2488.[22] It is also consistent with the elements of common-law fraud: "obtaining money or property by means of false or fraudulent pretenses, representation, or promises." *McNally*, 483 U.S. at 358.

The courts that have interpreted "intent to defraud" to mean "simply wrongdoing" have not taken this precedent and legislative guidance into account. *Shurgard Storage Centers v. Safeguard Self Storage, Inc.* appears to be the first case to take this approach, relying primarily on *Czubinski* to conclude—without analysis—that the term "fraud" within the CFAA "simply means wrongdoing and not proof of the common law elements of fraud." 119 F. Supp. 2d 1121, 1124 (E.D. Wa. 2000) (also citing *McNally,* 483 U.S. at 358 and *Hammerschmidt*, 265 U.S. at 199). Yet *Czubinski* interpreted the phrase "obtains anything of value" in subsection 1030(a)(4), not "intent to defraud." 106 F.3d at 1078. Other courts have subsequently relied upon *Shurgard* and *Czubinski* in finding that "intent to defraud" means "simply wrongdoing" for purposes of the CFAA, without considering the established meaning of "intent to defraud" as discussed in other cases or the CFAA's legislative history. *E.g.*, *Multiven*, 725 F. Supp. 2d at 892; *Hanger Prosthetics & Orthotics*, 556 F. Supp. 2d at 1131; *NCMIC Finance Corp. v. Artino*, 638 F. Supp. 2d 1042, 1062 (S.D. Iowa).

A narrow reading of "intent to defraud" is particularly critical because the CFAA is a criminal statute, and even first-time violations of subsection 1030(a)(4) are felonies. Interpreting

[22] Subsection 1030(a)(4) was expanded in 1996 to cover situations in which a malicious trespasser uses computer time worth more than $5,000 during any one-year period. While technically trespass, the Senate Judiciary Committee considered such scenarios to amount to "stolen computer use," consistent with protecting a property interest against theft. S. Rep. No. 104-357, 104th Cong., 2d Sess. (1996).

"intent to defraud" to mean "simply wrongdoing" would not give ordinary people notice about what behavior is criminal and would also "encourage arbitrary and discriminatory enforcement." *Skilling*, 130 S. Ct. at 2927-28 (quoting *Kolender*, 461 U.S. at 357 (internal quotation marks omitted)). Such a broad reading of the phrase creates void-for-vagueness concerns and threatens to render subsection 1030(a)(4) unconstitutional.

Applying the definition of "intent to defraud" that Congress intended, this Court should hold that Power did not have the requisite intent to "deceive another person, and to induce such other person, in reliance upon such deception, to assume, create, transfer, alter or terminate a right, obligation, or power with reference to property." Power did not deceive anyone: Facebook users knowingly chose to use Power's service to access their own accounts. And Facebook users—not Facebook—own the data in their accounts. At best, Facebook had a non-exclusive license to use that data. According to Facebook terms of use in place at the time Power accessed the Facebook site:

> By posting User Content to any part of the Site, you automatically grant . . . to the Company an irrevocable, perpetual, non-exclusive, transferable fully paid worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or part) and distribute such User Content for any purpose[.] . . . Facebook does not assert any ownership over your User Content, rather, as between us and you, subject to the rights granted to us in these Terms, you retain full ownership of all your User Content and any intellectual property rights or other proprietary rights associated with your User Content.

First Am. Compl. Ex. A (Dkt. No. 9-1). When Facebook users chose to use Power's tool to access their own information, they did not affect or disrupt any Facebook property right. Facebook still had access to the data under its non-exclusive license. Power also had permission to access the data at the direction of the property owner: the user. Thus, Power had no intent to defraud within the meaning of the CFAA.

5. A Calculation of "Loss" Under the CFAA Should Not Include Attorneys' Fees Related to Investigation or Initiation of a Lawsuit.

Facebook argues that it has standing to pursue a CFAA action under subsection 1030(g) because it incurred more than $5,000 in loss as a result of Power's tool. EFF does not have access

to the data underlying Facebook's calculation of loss, so cannot fully assess that argument. However, Power suggests that lawyers' fees are at least part of Facebook's basis for claiming loss. Power Reply ISO Power Mot. Summ. J. at 8:3-4 ("The only cost specifically identified in Facebook's motion is the money it paid its lawyer to investigate Power and to file this lawsuit.")

The CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.]" 18 U.S.C. § 1030(e)(11). Facebook cites dicta suggesting that costs for attorneys' time could count toward loss under certain circumstances. Facebook Reply ISO Mot. Partial Summ. J. § 502 & CFAA at 7:24-8:12, citing *Animators at Law v. Capital Legal Solutions, LLC*, 786 F. Supp. 2d 1114, 1118 (E.D. Va. 2010); *E.R. James Real Estate Services, LLC v. Spinell*, No. 11C4476, 2011 U.S. Dist. LEXIS 124044, *7 (N.D. Ill. Oct. 26, 2011). EFF urges the Court not to permit attorneys' fees and costs incurred while researching legal claims, drafting a cease-and-desist demand, or pursuing a lawsuit to be part of the basis for the $5,000 threshold for standing.

The text of the statute makes clear that "loss" includes costs directly tied to "responding to an offense" or "incurred because of interruption of service." The legislative history indicates that this definition was intended to include the cost of actual repairs, as well as those associated with lost computer time, reprogramming, and restoring data. S. Rep. No. 99-432, 1986 U.S.C.C.A.N. at 2489-90. But nothing in the statute or the legislative history indicates that costs associated with investigating legal claims, drafting demand letters and filing lawsuits are meant to be part of this calculation.

Indeed, allowing such attorneys' fees to count toward loss would give would-be litigants the power to manufacture standing. A lawyer considering a possible claim under the CFAA could easily generate $5,000 in fees researching legal arguments and drafting letters and pleadings—which itself would be adequate to create standing for a civil action under subsection 1030(g).

Even more troublingly, the $5,000 threshold for "loss" has consequences for other parts of

the statute, as well. For example, subsection 1030(a)(5) prohibits causing damage to a protected computer without authorization. Loss is an element of subsection 1030(a)(5)(C), which makes it unlawful to "intentionally access[] a protected computer without authorization, and as a result of such conduct, cause[] damage and loss." Under Facebook's theory, a person could violate subsection 1030(a)(5)(C) under circumstances in which the claimed "loss" involves nothing more than a computer owner tasking lawyers to investigate the possibility of filing a lawsuit, which could criminalize behavior that would otherwise not be unlawful at all.

Furthermore, subsection 1030(a)(5)(A) prohibits "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." Subsection 1030(a)(5)(B) makes it unlawful to "intentionally access[] a protected computer without authorization, and as a result of such conduct, recklessly cause[] damage." Causing $5,000 in loss is not an element of either offense, but can turn a misdemeanor violation of subsection 1030(a)(5)(A) or (B) into a felony. 18 U.S.C. §§ 1030(c)(4)(A)(i)(VI), (B)(i). Under Facebook's argument, a violation of either provision could result in stiff prison time even for first-time offenders if the computer owner spends enough time researching and drafting a demand letter about a possible civil claim.

Indeed, the United States Sentencing Guidelines provide that "loss" does not include costs incurred by victims primarily to assist law enforcement in investigating or prosecuting an offense. U.S.S.G. § 2B1.1, cmt. n.3(D)(ii); *United States v. Schuster*, 467 F.3d 614 (7th Cir. 2006). The rule should be the same for victims that investigate or initiate their own legal actions: these expenditures are not part of the "loss" calculation.

B. Facebook's Claims Under the CAN-SPAM Act Should Fail Because They are Based on the Service's Own Captive Message Generation Mechanism.

Facebook's claims under the CAN-SPAM Act are also dangerous, since they would give Facebook, or any other designer of a "captive" email generation program, the ability to invoke CAN-SPAM's powerful punitive provisions, including treble damages. Here, Facebook claims a staggering $18,188,100 in damages for alleged CAN-SPAM violations. The CAN-SPAM Act, which was passed in 2004 before the explosive growth of social networks and other captive

systems, was not intended to give email system designers who are also service providers the power to hold commercial users liable for crushing damages at their whim.

1. Neither Power Nor Users Can Control Key Elements of Messages Sent Through Facebook's "Events" Feature.

Facebook's claims under the CAN-SPAM Act, 15 U.S.C. §§ 7701, *et seq*., arise from Power's offer to its customers to use the "Events" feature that Facebook offers to invite their friends to try Power's service. "Events" are a Facebook "Popular Feature" that allow users to "Organize gatherings, respond to invites, and keep up with what your friends are doing." (https://www.facebook.com/help/events). As the name implies, Facebook's Events feature allows users to invite their Facebook friends to various events, both physical and virtual. Like most Facebook features, the Events feature is available to and utilized by Facebook users for commercial purposes.

Facebook's invitation mechanism for Events is not like a normal email program, however. It allows only certain information to be provided by the user, including the date, location and "friends" to be invited. The system does not allow changes to other key elements of the message and it automatically generates both internal invitation messages through Facebook's system and emails sent externally to those invited.

As a result, the very elements of the messages sent by Facebook's Events invitation mechanism that Facebook now claims are "materially false and misleading" are the elements of Events invitations that Facebook itself controls. This fact is obvious from Facebook's own example, on page 7:4-16 of its Corrected Motion for Partial Summary Judgment on Count 1 filed on November 18, 2011, and the "events" process screenshots that Power includes on pages 5-6 of its Motion for Summary Judgment filed on May 9, 2011. Those images reflect the following:

1) The "Create an Event" interface does not allow a user to change the "sender" field for either internal messages sent within Facebook or external messages sent via email over the public internet. Power Mot. Summ. J. at 5:9-28.

2) The invitations sent from Facebook's captive system externally read as coming from Facebook with a return address @facebookmail.com, regardless of who is actually organizing the Event. Facebook Corrected Mot. Partial Summ. J. on Count 1 at 7:4.

3) The invitations sent externally via email are signed in the text by "The Facebook Team," regardless of who is the sender or organizer of the event. Facebook Corrected Mot. Partial Summ. J. on Count 1 at 7:14-15.

4) The "Subject" line of the external emails includes the name of the Facebook user who has authorized the invitation to be sent, regardless of whether that user has actually "organized" the event. Facebook Corrected Mot. Partial Summ. J. on Count 1 at 7:5.

5) The message text of an internal message does name the organizer of the event, however, under the category "host." In Facebook's example, the email message clearly indicates that the "host" is Power. Facebook Corrected Mot. Partial Summ. J. on Count 1 at 7:10-11; Power Mot. Summ. J. at 9:15.

6) The external messages contain a notice on the bottom allowing recipients to "control which emails [they] receive from Facebook" with a link to a Facebook-hosted page that allows users to opt out of further invitations.

Internal Facebook messages provide even less information than external messages. They give no "return address" (but instead a hyperlink to the user's Facebook page), no "Subject" line, and no link to opt out. In the ordinary use of this feature, these attributes cannot be altered by any user, and so also could not have been altered by the user's agent, Power.

2. Because of its "Captive" Design Decisions, Facebook Should be Deemed the "Initiator" of the Messages for Purpose of the CAN-SPAM Act.

Facebook's legal arguments are only possible because the CAN-SPAM Act is based on a set of assumptions that simply are not applicable to Facebook's captive event invitation system. Under 15 U.S.C. § 7702(6), an "electronic mail message" is defined as a message sent to a unique

electronic mail address. The CAN-SPAM Act attaches obligations to any person that "initiates the transmission to a protected computer of a commercial electronic mail message." 15 U.S.C. §§ 7704(a)(1), (2), (3), and (5). By its terms, the statute presumes that all persons who can "initiate" email messages will have control over such items as the header information (subsection 7704(a)(1)), the subject heading (subsection 7704(a)(2)), the return address (subsection 7704(a)(3)), and the inclusion of identifiers, opt-outs and physical addresses (subsection 7704(a)(5)). But due entirely to Facebook's own design of its event and messaging systems, this is not true for messages sent via Facebook's Event invitation mechanism. The result is that any commercial user who utilizes Facebook's Event invitation mechanism is likely in violation of the CAN-SPAM Act under Facebook's interpretation of the law.

Power attempts to solve this problem by asserting that Facebook, not Power, is the "initiator" or sender of the messages for purposes of the CAN-SPAM Act. That analysis is reasonable given that Facebook, not Power, solely controls all elements of the messages that allegedly violate the CAN-SPAM Act. Facebook controls the From and Subject lines, requires the text to be signed "The Facebook Team," and includes links to its own system—not the user—for opt-out purposes. Given the design of the system, it is reasonable to find that Facebook is the "initiator" of the messages for purposes of CAN-SPAM liability, notwithstanding the user's (and her agent Power's) role in generating the specific messages sent. Any contrary decision would create legal chaos, as any designer of a captive messaging system could ensure that the messages it sends cannot comply with the CAN-SPAM Act and then, at its whim, hold any commercial user liable for CAN-SPAM violations merely by using the system. Here, Facebook is attempting to do just that for apparently anti-competitive purposes, but there would be no limitations on the use of this technique to punish users disfavored by the captive system creator.

3. Power is the Users' Agent for Purposes of the Event Invitations.

Facebook also claims that the process by which users gave Power access to their friends' lists on Facebook to generate the Event invitations is misleading. While EFF is not privy to all the discovery in this case, Power asserts that there is no evidence that any user was misled. Power Mot.

Summ. J. at 9:23-10:25. Facebook's own motion demonstrates that users were given a clear choice to participate in Power's promotion and clear notice that this would involve inviting their friends to an event. In its moving papers, Facebook includes the promotional pop-up window through which users created the event invitation. Facebook Corrected Mot. Partial Summ. J. on Count 1 at 5:13-23. A pre-checked box plainly and prominently notifies users that they will "Share with friends through events," and the box could be unchecked by users who did not wish to do so. Facebook makes much of the fact that Power automated that process so that its users did not have to manually invite all of their friends to the event or prepare the invitation text, but that automation alone should not trigger CAN-SPAM liability. All of the users who responded to Power's button could have manually invited all of their friends to Power's events; creating CAN-SPAM liability for their actions because Power automated this process would be unprecedented.

The unpublished cases Facebook relies upon are all easily distinguishable. In *Facebook, Inc. v. MaxBounty, Inc.*, the defendants allegedly tricked users into installing "malicious computer code." No. 5:10-cv-04712-JF (HRL), 2011 U.S. Dist. LEXIS 104055, *14 (N.D. Cal. Sept. 14, 2011). Nothing like that is alleged here. Power has asserted that no one was misled by its promotion and that conclusion is supported by review of the promotion itself.[23] And in *Federal Trade Commission v. AVATAR*, the court merely held that direct technical evidence that the defendant was the "sender" of the message was not necessary when significant circumstantial evidence indicated that it in fact was. No. 04C2897, 2004 U.S. Dist. LEXIS 14717 (N.D. Ill. July 30, 2004). In contrast, Power is not denying its role here; it is instead arguing that given how Facebook's captured system works, Facebook should be deemed to be the "initiator" of the messages for purposes of CAN-SPAM.

Similarly, Facebook relies on the fact that Power offered payments to Facebook users for agreeing to invite their friends. Yet this fact is irrelevant as to whether, given Facebook's creation of a captive message generation system, Power should be held as a "initiator" of the messages for

[23] At best, whether Power users were misled is an issue where there is a genuine issue of material fact preventing Facebook from obtaining summary judgment.

purposes of a finding that the messages generated by Facebook's system failed to comply with the CAN-SPAM Act.

VII. CONCLUSION

Based upon the foregoing, EFF respectfully requests that this Court grant summary judgment in favor of Power on Facebook's California Penal Code § 502(c), CFAA, and CAN-SPAM Act claims and deny Facebook's cross motions.

DATED: January 17, 2012

Respectfully submitted,

ELECTRONIC FRONTIER FOUNDATION

By */s/ Marcia Hofmann*

MARCIA HOFMANN
marcia@eff.org
CINDY A. COHN
cindy@eff.org
HANNI FAKHOURY
hanni@eff.org
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Fax: (415) 436-9993

Attorneys for *Amicus Curiae*
ELECTRONIC FRONTIER FOUNDATION

CERTIFICATE OF SERVICE

I hereby certify that on January 17, 2012, I electronically filed the foregoing document with the Clerk of the Court, using the CM/ECF system, which will send notification of such filing to the counsel of record in this matter who are registered on the CM/ECF system.

Executed on January 17, 2012, in San Francisco, California.

/s/ Marcia Hofmann
MARCIA HOFMANN